REMARKS/ARGUMENTS

Claims 1, 4, 5, 7, 8, 11-13, 15 and 17 are pending in the present application. Claims 1, 11 and 12 have been amended herewith. Reconsideration of the claims is respectfully requested.

I. 35 U.S.C. § 103, Obviousness

Claims 1, 4, 5, 7, 8, 11 and 12 stand rejected under 35 U.S.C. § 103 as being unpatentable over Holvey et al. (U.S. Publication No. 2004/0054935), hereinafter "Holvey" and Prihoda et al. (U.S. Patent No. 6,789,195), hereinafter "Prihoda" and further in view of Chadwick ("Smart Cards Aren't Always the Smart Choice," IEEE Computer, December 1999, v. 32, Issue 12, pp. 142-143), hereinafter "Chadwick". This rejection is respectfully traversed.

Per the features of Claim 1, a tiered encryption scheme is used that allows for protecting sensitive data for multiple users, whereby a table (the "user specific table") that contains information ("first data") used to decrypt the sensitive data (the "set") *is itself encrypted* – and thus two-levels of decryption are required for accessing the sensitive data (the "set), as decryption is performed on both the "user specific table" (in order to access the "first data") as well as the "set" (which is decrypted using the "first data" that was also decrypted). Importantly, this user specific table also contains location information ("second data") that is used to locate the sensitive data (the "set"), providing yet *an additional level of security* in that both the information used to decrypt the "set" (i.e., the "first data") as well as the information used to locate the "set" (i.e., the "second data") *are both encrypted* as they are both a part of the user specific table that is decrypted. In addition, the claimed 'token' has a two-pronged functionality, as it includes both (1) a means for authenticating the user, as well as (2) means for decrypting the "user specific table" (and such "user specific table" contains both the "first data" that is used to decrypt the "set" as well as "second data" that is used to locate the "set", as previously described hereinabove in the tiered-decryption discussion). None of the cited references teach either one of (1) tiered-decryption using a user specific table containing *both* decryption and location information for a 'set', or (2) a dual-functionality token, as will now be described in detail.

Claim 1 recites "means, responsive to successful authentication, for *decrypting* an encrypted user specific **table** associated with the user", "the user specific table comprises (i) first data associated with decryption of the set" and (ii) "second data associated with location of the set", and "wherein the means for accessing the set uses the first data to *decrypt* the set and the second data to *locate* the set" . As can be seen, and as previously described above, Claim 1 includes a tiered decryption scheme, where an encrypted user specific table is decrypted, and information ("first data" and "second data") in this user specific table is used to decrypt the "set" *as well as* locate the "set". Thus, both the user specific table as

well as the set are decrypted – and the user specific table includes both a "set" decrypter as well as a "set" locator, to advantageously provide an added level of security with respect to a user being able to access desired data (the "set") since both the decryption information ("first data"), as well as the location information ("second data"), must be decrypted in order to locate and access the "set".

In rejecting Claim 1, the Examiner acknowledges that Holvey does not disclose either one of (i) decrypting the user specific table, or (2) that such user specific table comprises data associated with decryption of the set. In an attempt to overcome these teaching deficiencies, the Examiner alleges that Prihoda teaches (i) decrypting a user specific table at col. 1, lines 57-65, and (ii) the user specific table comprises data associated with decryption of the set at col. 2, lines 15-20 and col. 3, lines 35-46 since a special key is described as being used for decrypting. Applicants urge that Prihoda does not describe decrypting a *user specific table* that includes both 'set' decryption information as well as 'set' location information. Instead, Prihoda describes use of a decryption key to assess sensitive data. This decryption key is not described as being maintained in a user specific table that must be decrypted in order to obtain access to the key. Instead, *this key is transmitted to an authorized users* (col. 31-33), where it is permanently kept by the user. Even to the extent this key may be transmitted in an encrypted form where it is subsequently decrypted for use in accessing encrypted data, the key is not maintained in a user specific table that also includes encrypted location information for a 'set' of data. Thus, it is urged that Claim 1 is not obvious in view of the cited references due to these missing claimed features that are not taught or suggested by the cited references.

Still further, and as alluded to above, the claimed 'token' has a two-pronged functionality, as it includes both (1) a means for authenticating the user, and (2) means for decrypting the "user specific table". None of the cited references teach a token have such dual-functionality. In rejecting this aspect of Claim 1, the Examiner cites Holvey's paragraph 22 and Prihoda's decryption key (col. 2, lines 15-16) as teaching such dual-functionality token. Applicants urge clear error, as this combined teaching describes one thing being used for one action (Holvey data access using either voice recognition or a password), and another thing being used for another action (Prihoda data access using a decryption key). Such combined teaching does not describe a *single thing ("token") having two different actions* ("means for authenticating the user" as well as "means for decrypting the user specific table" that includes *both* set decryption information *as well as* set location information). Thus, it is further urged that Claim 1 is not obvious in view of the cited references due to these missing claimed features that are not taught or suggested by the cited references.

Finally, and importantly, the above two distinctions synergistically co-act together to provide a unique security advantage in that a token having two distinct functions (authentication and decryption) is operable for invoking/enabling/accessing a given encrypted user specific table that protects both

decryption and location information for the ultimately protected data ("set") for each of a plurality of given users. It is therefore urged that Claim 1 is allowable in view of the cited references.

Applicants traverse the rejection of Claims 4, 5, 7 and 8 for reasons given above with respect to Claim 1 (of which Claims 4, 5, 7 and 8 depend upon).

Applicants traverse the rejection of Claims 11 and 12 for similar reasons to those given above with respect to Claim 1.

Therefore, the rejection of Claims 1, 4, 5, 7, 8, 11 and 12 under 35 U.S.C. § 103 has been overcome.

II. 35 U.S.C. § 103, Obviousness

Claims 13, 15 and 17 stand rejected under 35 U.S.C. § 103 as being unpatentable over the combination of Holvey and Prihoda as applied to Claim 1 above, and further in view of Mita et al (U.S. Publication No. 2002/0035485 A1), hereinafter "Mita". This rejection is respectfully traversed for similar reasons to those given above with respect to Claims 1, 11 and 12, respectively.

Therefore, the rejection of Claims 13, 15 and 17 under 35 U.S.C. § 103 has been overcome.

III. Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: October 16, 2008

Respectfully submitted,

/Wayne P. Bailey/

Wayne P. Bailey
Reg. No. 34,289
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Applicants